INFORMATION SECURITY AND CYBER SECURIY POLICY

The objective of the policy is to create a clear and comprehensive framework to protect the QNB Finansbank's assets, customer data and information systems against the cyber threats and to create a formal methodology for Information Security and Cyber Security activities carried out to identify and define security requirements, implement appropriate controls in order to minimize Information security risks, which is a part of QNB Finansbank's Information Security and Cyber Security Management process.

This policy summarizes its determination to establish and maintain a secure and resilient infrastructure against threats, to ensure the security of bank and customer information, and to maintain customer trust. The scope of this document is QNB Finansbank information assets, information systems infrastructure, employees and third party contractors.
Information is a valuable resource that is used in our processes and it exists in various environments. Protecting information has a great importance for QNB Finansbank.
The definition of Information Security in QNB Finansbank is; the protection of the information assets against threats to ensure business continuity and to minimize the financial and operational losses.

Our objective is to protect the confidentiality, integrity and availability of our information in use, at rest and in transit.

Information security and cyber security is managed risk based approach and planned, implemented and reviewed according global Information Security standards. The risk management approach includes the identification, evaluation, treatment of information security and cyber security risks and taking necessary measures. The bank manages information security and cyber security risks with an integrated risk management methodology in accordance with regulatory requirements, IS strategy and the bank's enterprise riskmanagement framework at an acceptable tolerance level for the business.

Board of Directors is ultimately responsible to ensure the information security across the Bank. The board of directors is obliged to show the necessary determination to get the security measures related to information systems to the appropriate level and to allocate sufficient resources for the activities to be carried out for this purpose. Within the scope of this responsibility, the board of directors establishes an information security management system that it is responsible for overseeing its implementation across the Bank. The information security management system references national or international standards.

It is ensured that the bank's general cyber security strategy is established, adequate resources are provided and the effectiveness of cyber security measures is regularly reviewed. In order to ensure the confidentiality, integrity and availability of information assets, effective controls are established on information systems, and an effective monitoring activity is carried out to manage the risks arising from the use of information systems, taking into account the developing new technologies. How the information security management system will be implemented throughout the bank is regulated by the information security and cyber security policy, procedures and process documents. Acceptable usage standarts for information system are determined.

In order to establish appropriate controls to the security requirements of information assets, the Bank classifies these assets and prepares a detailed asset inventory. It is ensured that each asset has a defined and approved security class and access restriction. Appropriate protection of information assets against misuse and damage is ensured against the risks associated with security breaches affecting the confidentiality, integrity and availability of assets.

Classification and labeling of data according to the security class is provided. Measures are taken to ensure its confidentiality, regardless of whether the environment in which it is kept is paper or electronic media in the environments where data is transported, transmitted, processed, stored and kept as a backup according to the security class, Data sharing conditions are determined. It is essential to use end-to-end secure communication in the transmission of sensitive data between environments with different security levels and to store this data in an encrypted manner. For the encryption techniques to be used to ensure data confidentiality, algorithms that have not lost their reliability as of the current situation and are suitable for today's technology are used. Destruction policies and conditions in accordance with the degree of confidentiality of the data contained in environments, media or devices containing data are determined and they are safely destroyed. Information owners are the business unit representatives who have the ultimate authority and responsibile to ,classification of information asset, granting access,decide on when and how to update, delete, transfer and dispose their information.

The Bank is obliged to ensure that access to information assets is carried out with an authentication method in accordance with the security class of the associated information asset, in accordance with the access controls defined for the responsibility of the users, determined according to the principle of segregation of duties and least authority. Authentication and access management policies and standards for information systems are determined.

The Bank takes the necessary measures to ensure the integrity of transactions, records and data carried out through information systems and ensures their accuracy, integrity and reliability. In project management, security requirements are determined and met in the project life cycle.

Legal requirements, security and confidentiality requirements such as authentication, authorization, access controls, approval mechanisms, encryption, trace recording, and detailed requirements for integrity and availability are defined.

The Bank establishes an effective log management mechanism for transactions and events taking place within the information systems. Details, contents, storage period, access, follow-up conditions of logs are defining according the risks and legal requirements. Log management mechanism shall be ensured that to be established is of a quality that will allow the subsequent investigation of the information security and cyber security incidents and the obtaining of reliable evidence about them.

The cyber security architecture which summarizes the bank's cyber security solutions and requirements and addresses design principles for the development of cyber security capabilities within the corporate architecture is defined. Investments are made in state-of-the-art security tools and technologies to provide protection against advanced and current threats in line with the created security strategy. The bank establishes the necessary network security control systems for threats from both its own corporate network and external networks. The establishment of security measures is based on a multi-layered security architecture. Security configuration management is provided for the operating system, database, applications and network devices. An effective vulnerability and threat management process, patch management process is established in order to detect potential security vulnerabilities and threats in the bank's IT infrastructure and processes, and to resolve them quickly and effectively. Comprehensive and regular risk assessment, penetration tests and security scans are carried out.

INFORMATION SECURITY AND CYBER SECURIY POLICY

The Bank establishes an effective cyber incident management and response to cyber incidents for the detection, handling, tracking and reporting of cyber incidents, resolving the incident in a way that will affect the banking activities the least and to return the IT services to their normal functioning as soon as possible.

An adequate oversight mechanism is established for the assessment and management of the security risks posed by the services to be received from outsource services and suppliers for the bank.

In order to prevent unauthorized access and intervention against external and environmental threats to bank facilities, data center, critical information systems and assets, physical security controls are established in line with legal requirements, and relevant policies and standards are determined.

The Bank uses techniques that make it possible to assign responsibility and undeniability for both the bank and the customer in the transactions carried out within the scope of the electronic banking services it offers. Authentication and transaction security policies are determined and implemented. Appropriate security measures are taken regarding threats and cyber security risks related to electronic banking services, technological solutions are used, necessary patches and updates are made available to customers to eliminate security vulnerabilities. The security principles adapted by the bank to reduce the impact of risks related to electronic banking services and the methods to be used to avoid these risks are presented to the attention of the customer.

Information Technologies Executive Vice President is responsible for adequate management and protection of the information and its environments on which it resides in accordance with the security requirements defined by the information owners.

All of the employees and third party contractors are responsible to comply with relevant laws and regulations, banking laws in our country, BRSA regulations and this policy. Thus, all information and information systems users and administrators are required to;

- ✓ Protect the confidentiality, integrity and availability of information assets,
- ✓ Be aware and implement the information security and cyber security policy, standards, procedures and directions,
- ✓ Use IT resources in compliance with the laws, policies and business objectives,
- ✓ Ensure the confidentiality and privacy of customer information,
- ✓ Comply with the clear desk and clear screen policy,
- ✓ Share information only with authorized people,
- ✓ Use strong passwords and ensure their confidentiality,
- ✓ Ensure proper back-up of information and business continuity,
- ✓ Classify their information and ensure the implementation of the necessary controls,
- ✓ Report the information security incidents and the potential security weaknesses.

Top management is responsible to support activities in order to improve the security awareness for all employees, service providers and customers and provide necessary resources to protect information Bank creates and implements a comprehensive information security training program to increase the Information Security and cyber security awareness across the Bank.

Top management is also responsible for supervision of the information security and cyber security controls and enforcement of the disciplinary process in case of a security violation.

INFORMATION SECURITY AND CYBER SECURIY POLICY

The “Information Security and Cyber Security Committee” provides direction and coordination for the information security and cyber security efforts, oversees the development of the information security and cyber security policy and the implementation of the information security management on behalf of the top management. The Committee monitors and reviews information security and cyber security strategy, policies, programs, security risk management process, key risk indicators (KRIs) and key performance indicators (KPIs), and reports to the board of directors at least once a year regarding the activities carried out.

It is mandatory that Bank’s information security and cyber security practices are in compliance with group cyber security policies and underlines our commitment to the shared vision of maintaining a secure and resilient digital environment across the group. It is aimed to remain resilient against cyber threats and build confidence in our bank's security capabilities by implementing proactive measures across all groups and subsidiaries, constantly monitoring the security environment, and encouraging a cybersecurity-sensitive culture. This approach provides consistency, collaboration and collective strength in protecting our digital assets, customer data and critical systems.

Compliance with information security and cyber security policy is audited by Internal Audit Department and reported to top management. Internal Audit Department conducts internal investigations in case of information security policy violations and the perpetrators are sanctioned in accordance with the verdicts of the disciplinary board.

This policy is reviewed periodically at least once a year by the Board of Directors. Changes in laws and regulations, significant information security incidents, new critical vulnerabilities or changes in information security requirements as a result of the significant infrastructure changes require the review of the policy. Reviewed policy is approved and published in electronic environment to be made available to the appropriate audience.